FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY DOCKET NO.	SERIAL NO.
	20206-25	09/328,726
INFORMATION DISCLOSURE STATEMENT BY APPLICATED	APPLICANT	
OIPE VO	Collins	
007 0 2 7000 28	FILING DATE	GROUP
\\	October 26, 1998	2766
TO CHARLES		

## U. S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						

## FOREIGN PATENT DOCUMENTS

ſ	DOCUMENT NUMBER	DATE	COUNTRY	NAME	CLASS	SUBCLASS	TRANSLATION YES NO	
ľ								

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

AC RSA '98 Presentation – F. Levy-dit-Vehel – January 98 "Stuffing An RSA Into The Smallest 68HC05", pp. 1-14.  AD Generating a Product of Three Primes With an Unknown Factorization, Dan Bonch and Jeremy Horwitz, Computer Sc Department, Stanford University.  AE ChipCenter: The Web's Definitive Electronics Resource – "Compaq Computer Corporation – WebScan: Press Release (411/00)  AF Newell Public Relations, Hong Kong – "RSA Security teams with Compaq to provide high-speed cryptography breakthrough for manufacturers of wireless and embedded devices" (April 19, 2000)  AG Compaq News via WebLibrary – "New RSA BSAFE Crypto-C Encryption Software Offers up to 500 Percent Performan Gains for E-Commerce, Secure E-Mail and Other Applications" PR News Wire via DowVision (September 6, 2000).  Compaq News via WebLibrary – "RSA Security Releases RSA Encryption Algorithm into Public Domain" PR News Wire 10 Dowlession (September 6, 2000).  Compaq News via WebLibrary – "RSA Security Releases RSA Encryption Algorithm into Public Domain" PR News Wire 10 Dowlession (September 6, 2000).  Compaq News via WebLibrary – "RSA Security Releases RSA Encryption Algorithm into Public Domain" PR News Wire 10 Dowlession (September 6, 2000).  Compaq News via WebLibrary – "RSA Security Feleases RSA Encryption Algorithm into Public Domain" PR News Wire 10 Dowlession (September 6, 2000).  Compaq News via WebLibrary – "RSA Security Releases RSA Encryption Algorithm into Public Domain" PR News Wire 10 Dowlession (September 6, 2000).  Compaq News via WebLibrary – "RSA Security Feleases RSA Encryption Algorithm into Public Domain" PR News Wire 10 Dowlession (September 6, 2000).  Compaq News via WebLibrary – "RSA Security Feleases RSA Encryption Algorithm into Public Domain" PR News Wire 10 Dowlession (September 6, 2000).  Compaq News via WebLibrary – "RSA Security Feleases RSA Encryption Algorithm into Public Dowless of Compage RSA Security Proceedings RSA Encryption Algorithm into Public Res Algorithm into Public Res Algorithm into Public Res Algor	pwk	AB	IEEE 1994 Electronics Letters Online No: 19941450 "Using four-prime RSA in which some of the bits are specified" S. A. Vanstone and R. J. Zuccherat – Electronics Letters 8th December 1994 Vol 30, No. 24, pp. 2118, 2119.
Generating a Product of Three Primes With an Unknown Factorization, Dan Bonch and Jeremy Horwitz, Computer Sc Department, Stanford University.     Pwk   AE			RSA '98 Presentation - F. Levy-dit-Vehel - January 98 "Stuffing An RSA Into The Smallest 68HC05", pp. 1-14.
PWK   AF   Newell Public Relations, Hong Kong - "RSA Security teams with Compaq to provide high-speed cryptography breakthrough for manufacturers of wireless and embedded devices" (April 19, 2000)   PWK   AG   Compaq News via WebLibrary - "New RSA BSAFE Crypto-C Encryption Software Offers up to 500 Percent Performant Gains for E-Commerce, Secure E-Mail and Other Applications" PR News Wire via DowVision (September 6, 2000).   PWK   AH   Compaq News via WebLibrary - "RSA Security Releases RSA Encryption Algorithm into Public Domain" PR News Wia DowVision (September 6, 2000).   PWK   AI   RSA Security - RSA BSAFE* - Wireless Transport Layer Security for C (8/31/2000).   AJ   CyberLaw Presents: The RSA Algorithm & The RSA Patent - "Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?" Patrick J. Flinn and James Jordan III*; (c) 1997 Alston & Bird LLP (July 9, 1997).   PWK   RSA Laboratories / Bulletin 13 (April 2000) "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Length Robert D. Silverman, RSA Laboratories   PWK   RSA Laboratories / Bulletin 13 (April 2000) "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Length Robert D. Silverman, RSA Laboratories   PWK   AM   Lecture Notes in Computer Science (Edited by G. Goos and J. Hartmanis) - "Advances in Cryptology - CRYPTO '86"   Proceedings   Proceedings   "An Introduction to Fast Generation of Large Prime Numbers" by C. Couvreur and J. J. Quisquater; Phillips J. Res. 37   231-264, 1982   AO   "A Method for Obtaining Digital Signatures and Public Key Cryposystems" R. L. Rivest, A. Shamir, and L. Adelman, Laboratory for Computer Science and Department of Mathematics As Intractable As Factorization" Michael O. Ra (January 1979) Massachusetts Institute of Technology Laboratory for Computer Science.   Permutation Polynomials in RSA-Cryptosystems Rudolf Lidl and Winfried B. Müller; Department of Mathematics, Universität Klagenfurt, A-9020 Klagenfurt Austr	,	AD	Generating a Product of Three Primes With an Unknown Factorization, Dan Boneh and Jeremy Horwitz, Computer Science Department, Stanford University.
breakthrough for manufacturers of wireless and embedded devices." (April 19, 2000)  Compaq News via WebLibrary - "New RSA BSAFE Crypto- Encryption Software Offers up to 500 Percent Performant Gains for E-Commerce, Secure E-Mail and Other Applications." PR News Wire via DowVision (September 6, 2000).  All Compaq News via WebLibrary - "RSA Security Releases RSA Encryption Algorithm into Public Domain." PR News Wis DowVision (September 6, 2000).  All RSA Security - RSA BSAFE* - Wireless Transport Layer Security for C (8/31/2000).  CyberLaw Presents: The RSA Algorithm & The RSA Patent - "Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?" Patrick J. Flinn and James Jordan Ill*; (c) 1997 Alston & Bird LLP (July 9, 1997).  AK RSA Laboratories / Bulletin 13 (April 2000) "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Length Robert D. Silverman, RSA Laboratories (Califed by G. Gaos and J. Hartmanis) - "Advances in Cryptology - CRYPTO '86"  Proceedings  AM Lecture Notes in Computer Science (Edited by G. Gaos and J. Hartmanis) - "Advances in Cryptology - CRYPTO '86"  Proceedings  AN "An Introduction to Fast Generation of Large Prime Numbers" by C. Couvreur and J. J. Quisquater; Phillips J. Res. 37  231-264, 1982  AO "A Method for Obtaining Digital Signatures and Public Key Cryposystems" R. L. Rivest, A. Shamir, and L. Adelman, Laboratory for Computer Science and Department of Mathematics  AP MITILESTR-212 - "Digitalized Signatures and Public-Key Functions As Intractable As Factorization" Michael O. Ra  (January 1979) Massachusetts Institute of Technology Laboratory for Computer Science.  University of Tasmania, Hobart Australia 7001 and Institut für Mathematik, Universität Klagenfurt, A-9020 Klagenfurt  Austria	pwk	AE	(4/11/00)
Gains for E-Commerce, Secure E-Mail and Other Applications "PR News Wire via DowVision (September 6, 2000).  PWK  AH  Compaq News via WebLibrary - "RSA Security Releases RSA Encryption Algorithm into Public Domain" PR News W via DowVision (September 6, 2000).  AL  RSA Security - RSA BSAFE* - Wireless Transport Layer Security for C (8/31/2000).  CyberLaw Presents: The RSA Algorithm & The RSA Patent - "Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?" Patrick J. Flinn and James Jordan III*; (c) 1997 Alston & Bird LLP (July 9, 1997).  RSA Laboratories / Bulletin 13 (April 2000) "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Length Robert D. Silverman, RSA Laboratories  Robert D. Silverman, RSA Laboratories  Pokk  AL  1982 International Symposium on Information Theory; Les Arcs, France (June 21-25, 1982).  Lecture Notes in Computer Science (Edited by G. Gaos and J. Hartmanis) - "Advances in Cryptology - CRYPTO '86"  Proceedings  "An Introduction to Fast Generation of Large Prime Numbers" by C. Couvreur and J. J. Quisquater; Phillips J. Res. 37  231-264, 1982  "An Method for Obtaining Digital Signatures and Public Key Cryposystems" R. L. Rivest, A. Shamir, and L. Adelman, Laboratory for Computer Science and Department of Mathematics  AP  MIT/LCS/TR-212 - "Digitalized Signatures and Public-Key Functions As Intractable As Factorization" Michael O. Ra  (January 1979) Massachusetts Institute of Technology Laboratory for Computer Science.  Permutation Polynomials in RSA-Cryptosystems Rudolf Lidl and Winfried B. Müller; Department of Mathematics, University of Tasmania, Hobart Australia 7001 and Institut für Mathematik, Universität Klagenfurt, A-9020 Klagenfurt  Austria	pwk	AF	breakthrough for manufacturers of wireless and embedded devices" (April 19, 2000)
Compaq News via WebLibrary - "RSA Security Releases RSA Encryption Algorithm into Public Domain" PR News W via DowVision (September 6, 2000).  RSA Security - RSA BSAFE* - Wireless Transport Layer Security for C (8/31/2000).  CyberLaw Presents: The RSA Algorithm & The RSA Patent - "Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?" Patrick J. Flinn and James Jordan III*; (c) 1997 Alston & Bird LLP (July 9, 1997).  RSA Laboratories / Bulletin 13 (April 2000) "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Length Robert D. Silverman, RSA Laboratories Proceedings  AM 1982 International Symposium on Information Theory: Les Arcs, France (June 21-25, 1982).  Lecture Notes in Computer Science (Edited by G. Goos and J. Hartmanis) - "Advances in Cryptology - CRYPTO '86" Proceedings  "An Introduction to Fast Generation of Large Prime Numbers" by C. Couvreur and J. J. Quisquater; Phillips J. Res. 37 231-264, 1982  "A Method for Obtaining Digital Signatures and Public Key Cryposystems" R. L. Rivest, A. Shamir, and L. Adelman, Laboratory for Computer Science and Department of Mathematics  MITILESTR-212 - "Digitalized Signatures and Public-Key Functions As Intractable As Factorization" Michael O. Ra (January 1979) Massachusetts Institute of Technology Laboratory for Computer Science.  Permutation Polynomials in RSA-Cryptosystems Rudolf Lidl and Winfried B. Müller; Department of Mathematics, University of Tasmania, Hobart Australia 7001 and Institut für Mathematik, Universität Klagenfurt, A-9020 Klagenfurt, Australia	pwk	AG	Compaq News via WebLibrary - "New RSA BSAFE Crypto-C Encryption Software Offers up to 500 Percent Performance Gains for E-Commerce, Secure E-Mail and Other Applications" PR News Wire via DowVision (September 6, 2000).
All RSA Security - RSA BSAFE* - Wireless Transport Layer Security for C (8/31/2000).  All CyberLaw Presents: The RSA Algorithm & The RSA Patent - "Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?" Patrick J. Flinn and James Jordan III*; (c) 1997 Alston & Bird LLP (July 9, 1997).  AK RSA Laboratories / Bulletin 13 (April 2000) "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Length Robert D. Silverman, RSA Laboratories  Robert D. Silverman, RSA Laboratories  I 1982 International Symposium on Information Theory; Les Arcs, France (June 21-25, 1982).  Lecture Notes in Computer Science (Edited by G. Gaos and J. Hartmanis) - "Advances in Cryptology - CRYPTO '86"  Proceedings  "An Introduction to Fast Generation of Large Prime Numbers" by C. Couvreur and J. J. Quisquater; Phillips J. Res. 37  231-264, 1982  "A Method for Obtaining Digital Signatures and Public Key Cryposystems" R. L. Rivest, A. Shamir, and L. Adelman, Laboratory for Computer Science and Department of Mathematics  AP MIT/LCS/TR-21/2 - "Digitalized Signatures and Public-Key Functions As Intractable As Factorization" Michael O. Ra (January 1979) Massachusetts Institute of Technology Laboratory for Computer Science.  Permutation Polynomials in RSA-Cryptosystems Rudolf Lidl and Winfried B. Müller; Department of Mathematics, University of Tasmania, Hobart Australia 7001 and Institut für Mathematik, Universität Klagenfurt, A-9020 Klagenfurt, A-9020 Klagenfurt	-	AH	Compaq News via WebLibrary - "RSA Security Releases RSA Encryption Algorithm into Public Domain" PR News Wire
Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?" Patrick J. Flinn and James Jordan Ill*; (c) 1997 Alston & Bird LLP (July 9, 1997).  RSA Laboratories / Bulletin 13 (April 2000) "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Length Robert D. Silverman, RSA Laboratories  Ro		AJ	RSA Security - RSA BSAFE* · Wireless Transport Layer Security for C (8/31/2000).
Robert D. Silverman, RSA Laboratories  AL . 1982 International Symposium on Information Theory; Les Arcs, France (June 21-25, 1982).  Lecture Notes in Computer Science (Edited by G. Goos and J. Hartmanis) - "Advances in Cryptology - CRYPTO '86"  Proceedings  AN . "An Introduction to Fast Generation of Large Prime Numbers" by C. Couvreur and J. J. Quisquater; Phillips J. Res. 37 231-264, 1982  AO . "A Method for Obtaining Digital Signatures and Public Key Cryposystems" R. L. Rivest, A. Shamir, and L. Adelman, Laboratory for Computer Science and Department of Mathematics  MIT/LCS/TR-212 - "Digitalized Signatures and Public-Key Functions As Intractable As Factorization" Michael O. Ra (January 1979) Massachusetts Institute of Technology Laboratory for Computer Science.  Permutation Polynomials in RSA-Cryptosystems Rudolf Lidl and Winfried B. Müller; Department of Mathematics, University of Tasmania, Hobart Australia 7001 and Institut für Mathematik, Universität Klagenfurt, A-9020 Klagenfurt Austria		AJ	Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?" Patrick J. Flinn and James M.
PWK AL	lwk	AK	RSA Laboratories / Bulletin 13 (April 2000) "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths" Robert D. Silverman, RSA Laboratories
Proceedings  AN  AN  AN  AN  AN  AN  AN  AN  AN  A		AL	. 1982 International Symposium on Information Theory; Les Arcs, France (June 21-25, 1982).
Wk   AN   "An Introduction to Fast Generation of Large Prime Numbers" by C. Couvreur and J. J. Quisquater; Phillips J. Res. 37   231-264, 1982   "A Method for Obtaining Digital Signatures and Public Key Cryposystems" R. L. Rivest, A. Shamir, and L. Adelman, Laboratory for Computer Science and Department of Mathematics   MIT/LCS/TR-212 - "Digitalized Signatures and Public-Key Functions As Intractable As Factorization" Michael O. Ra (January 1979) Massachusetts Institute of Technology Laboratory for Computer Science.    AQ   Permutation Polynomials in RSA-Cryptosystems Rudolf Lidl and Winfried B. Müller; Department of Mathematics, University of Tasmania, Hobart Australia 7001 and Institut für Mathematik, Universität Klagenfurt, A-9020 Klagenfurt, Austria		AM	
## AMETHOD For Obtaining Digital Signatures and Public Key Cryposystems" R. L. Rivest, A. Shamir, and L. Adelman, Laboratory for Computer Science and Department of Mathematics  ### APP   MITI/LCS/TR-212 - "Digitalized Signatures and Public-Key Functions As Intractable As Factorization" Michael O. Ra (January 1979) Massachusetts Institute of Technology Laboratory for Computer Science.  #### APP   MITI/LCS/TR-212 - "Digitalized Signatures and Public-Key Functions As Intractable As Factorization" Michael O. Ra (January 1979) Massachusetts Institute of Technology Laboratory for Computer Science.  ###################################		AN	231-264, 1982
AP  MIT/LCS/TR-212 - "Digitalized Signatures and Public-Key Functions As Intractable As Factorization" Michael O. Ra (January 1979) Massachusetts Institute of Technology Laboratory for Computer Science.  Permutation Polynomials in RSA-Cryptosystems Rudolf Lidl and Winfried B. Müller; Department of Mathematics, University of Tasmania, Hobart Australia 7001 and Institut für Mathematik, Universität Klagenfurt, A-9020 Klagenfurt Austria		AO	Laboratory for Computer Science and Department of Mathematics
Permutation Polynomials in RSA-Cryptosystems Rudolf Lidl and Winfried B. Müller; Department of Mathematics, University of Tasmania, Hobart Australia 7001 and Institut für Mathematik, Universität Klagenfurt, A-9020 Klagenfurt Austria		AP	(January 1979) Massachusetts Institute of Technology Laboratory for Computer Science.
A I AR . PKCS #1: RSA Encryption Standart - An RSA Laboratories Technical Note, Version 1.5. Revised November 1, 1993		AQ	University of Tasmania, Hobart Australia 7001 and Institut für Mathematik, Universität Klagenfurt, A-9020 Klagenfurt, Austria
THAT I I I I I I I I I I I I I I I I I I I	pwt.	AR	- PKCS #1: RSA Encryption Standart - An RSA Laboratories Technical Note, Version 1.5, Revised November 1, 1993

(Form PTO-1449) SV/107356.01 09272000/12:41/20206.25

	on Cetin Kaya Koc, RSA Laboratories RSA Data Security, Inc., 100 Marine Parkway, Suite 5-1031; Copyright ♥ RSA Laboratories Version 2.0 – November 1994
() (°)	
Paula Klimach OCT 0 2 2000	DATE CONSIDERED
EXAMINER: Initial if citation considered, whether multi-citation is in considered. Include copy of this form with next communication to applica	nformance with MPEP 609; draw line through citation if not in conformance and not nt.

(Form PTO-1449) SV/107356.01 09272000/12:41/20206.25